Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method comprising:

associating each workflow of a plurality of workflows with a corresponding domain of a plurality of domains in an Identity System, each domain of said plurality of domains comprising one or more entities and each workflow of said plurality of workflows using a different predefined set of steps to perform a certificate related action affecting validity of the certificate, the certificate comprising a security credential, wherein each workflow in said plurality of workflows corresponds to a different set of characteristics for a user, wherein the first workflow contains a first set of steps and a second workflow in said plurality of workflows contains a second set of steps, wherein said first set of steps is different from said second set of steps, wherein said first workflow calls for obtaining an approval before performing a certificate related action for users having a first user type, and wherein said second workflow does not call for obtaining an approval before performing a certificate related action for users having a second user type;

receiving at the Identity System a request for a first certificate related action for a first user wherein the first certificate related action is selected from a group consisting of a certificate enrollment action, a certificate renewal action, and a certificate revocation action;

determining from said plurality of domains a domain that includes said user;

determining from said plurality of workflows, one or more workflows associated with said domain and capable of performing said certificate related action;

retrieving by the Identity System from said one or more workflows associated with said domain a first workflow for responding to said request wherein retrieving the first workflow comprises selecting the first workflow from the one or more workflows associated with said domain based on the first certificate related action and a user type of the first user from

a set of characteristics for the first user from an identity profile for the first user maintained by the Identity System being the first user type and wherein the request includes an identification of said identity profile for the first user;

performing said first workflow, wherein performing said first workflow comprises executing said predefined set of steps of said first workflow to perform said certificate related action including retrieving an approval response from an entity associated with the first user and identified in the identity profile for the first user and obtaining a certificate and a real time status for the certificate from a certificate authority based on the approval response; and

storing the certificate and said real time status in the Identity System, wherein the certificate authority is external to the Identity System.

2.-6. (Canceled)

7. (Previously Presented) The method of claim 1, further comprising:

receiving said plurality of workflows.

8. (Canceled)

9. (Previously Presented) The method of claim 1, further comprising:

receiving at the Identity System a second request for a second certificate related action for a second user wherein the second certificate related action is selected from a group consisting of a certificate enrollment action, a certificate renewal action, and a certificate revocation action;

determining by the Identity System from said plurality of domains a domain that includes said second user;

determining by the Identity System from said plurality of workflows, one or more workflows associated with said domain that includes said second user and capable of performing said second certificate related action;

retrieving by the Identity System from said one or more workflows associated with said domain that includes the second user a second workflow for responding to said second

request, wherein retrieving the second workflow further comprises selecting the second workflow from the one or more workflows associated with said domain that includes said second user based on the second certificate related action and a user type of the second user from a set of characteristics for the second user from an identity profile for the second user maintained by the Identity System being the second user type, and wherein the second request includes an identification of said identity profile of the second user; and

performing said second workflow, wherein performing said second workflow comprises executing said predefined set of steps of said second workflow to perform said certificate related action including obtaining a second certificate without retrieving an approval response.

10. (Previously Presented) The method of claim 9, wherein said first certificate related action is a certificate enrollment action and said second certificate related action is a certificate enrollment action.

11. (Previously Presented) The method of claim 9, wherein said first certificate related action is a certificate renewal action and said second certificate related action is a certificate renewal action.

12. (Previously Presented) The method of claim 1, further comprising:

performing said first workflow, wherein said first certificate related action is a certificate enrollment action and wherein performing said first workflow comprises:

obtaining a certificate, wherein obtaining the certificate comprises

authenticating said first user;

forwarding said request to a Certificate Processing Server;

receiving said certificate; and

storing said certificate.

13. (Previously Presented) The method of claim 1, further comprising:

performing said first workflow, wherein said first certificate related action is a certificate renewal action and wherein performing said first workflow comprises:

obtaining a certificate renewal, wherein obtaining the certificate renewal comprises:

authenticating said first user;

forwarding said request to a Certificate Processing Server;

receiving a certificate renewal acknowledgement.

14. (Previously Presented) The method of claim 1, further comprising:

performing said first workflow, wherein said first certificate related action is a certificate revocation action and wherein performing said first workflow comprises:

revoking a certificate, wherein revoking the certificate comprises:

authenticating said first user; and

forwarding said request to a Certificate Processing Server.

15. (Canceled)

16. (Currently Amended) One or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising:

associating each workflow of a plurality of workflows with a corresponding domain of a plurality of domains in an Identity System, each domain of said plurality of domains comprising one or more entities and each workflow of said plurality of workflows using a different predefined set of steps to perform a certificate related action affecting validity of the certificate, the certificate comprising a security credential, wherein each workflow in said plurality of workflows corresponds to a different set of characteristics for a user, wherein the first workflow contains a first set of steps and a second workflow in said plurality of workflows contains a second set of steps, wherein said first set of steps is different from said second set of

steps, wherein said first workflow calls for obtaining an approval before performing a certificate related action for users having a first user type, and wherein said second workflow does not call for obtaining an approval before performing a certificate related action for users having a second user type;

receiving at the Identity System a request for a first certificate related action for a first user wherein the first certificate related action is selected from a group consisting of a certificate enrollment action, a certificate renewal action, and a certificate revocation action;

determining from said plurality of domains a domain that includes said user;

determining from said plurality of workflows, one or more workflows associated with said domain and capable of performing said certificate related action;

retrieving by the Identity System from said one or more workflows associated with said domain a first workflow for responding to said request wherein retrieving the first workflow comprises selecting the first workflow from the one or more workflows associated with said domain based on the first certificate related action and a user type of the first user from a set of characteristics for the first user from an identity profile for the first user maintained by the Identity System being the first user type and wherein the request includes an identification of said identity profile for the first user;

performing said first workflow, wherein performing said first workflow comprises executing said predefined set of steps of said first workflow to perform said certificate related action including retrieving an approval response from an entity associated with the first user and identified in the identity profile for the first user and obtaining a certificate and a real time status for the certificate from a certificate authority based on the approval response; and

storing the certificate and said real time status in the Identity System, wherein the certificate authority is external to the Identity System.

17.-19. (Canceled)

20. (Previously Presented) One or more processor readable storage devices according to claim16, wherein said method further comprises:

receiving said plurality of workflows.

21. (Previously Presented) One or more processor readable storage devices according to claim 16, wherein said method further comprises:

receiving at the Identity System a second request for a second certificate related action for a second user wherein the second certificate related action is selected from a group consisting of a certificate enrollment action, a certificate renewal action, and a certificate revocation action;

determining by the Identity System from said plurality of domains a domain that includes said second user;

determining by the Identity System from said plurality of workflows, one or more workflows associated with said domain that includes said second user and capable of performing said second certificate related action;

retrieving by the Identity System from said one or more workflows associated with said domain that includes the second user a second workflow for responding to said second request, wherein retrieving the second workflow further comprises selecting the second workflow from the one or more workflows associated with said domain that includes said second user based on the second certificate related action and a user type of the second user from a set of characteristics for the second user from an identity profile for the second user maintained by the Identity System being the second user type, and wherein the second request includes an identification of said identity profile of the second user; and

performing said second workflow, wherein performing said second workflow comprises executing said predefined set of steps of said second workflow to perform said certificate related action including obtaining a second certificate without retrieving an approval response.

22. (Previously Presented) One or more processor readable storage devices according to claim 21, wherein said first certificate related action is a certificate enrollment action and said second certificate related action is a certificate enrollment action.

23. (Previously Presented) One or more processor readable storage devices according to claim 16, wherein said method further comprises:

performing said first workflow, wherein said first certificate related action is a certificate enrollment action and wherein performing said first workflow comprises:

obtaining a certificate, wherein obtaining the certificate comprises:

authenticating said first user;

forwarding said request to a Certificate Processing Server;

receiving said certificate; and

storing said certificate.

24. (Previously Presented) One or more processor readable storage devices according to claim 16, wherein said method further comprises:

performing said first workflow, wherein said first certificate related action is a certificate renewal action and wherein performing said first workflow comprises:

obtaining a certificate, wherein obtaining the certificate comprises

authenticating said first user;

forwarding said request to a Certificate Processing Server; and

receiving a certificate renewal acknowledgement.

25. (Previously Presented) One or more processor readable storage devices according to claim 16, wherein said method further comprises:

performing said first workflow, wherein said first certificate related action is a certificate revocation action and wherein performing said first workflow comprises:

revoking a certificate, wherein revoking the certificate comprises:

authenticating said first user; and

forwarding said request to a Certificate Processing Server.

26. (Canceled)

27. (Currently Amended) An apparatus comprising:

one or more communications interfaces;

one or more storage devices; and

one or more processors in communication with said one or more storage devices and said one or more communication interfaces, said one or more processors perform a method comprising:

associating each workflow of a plurality of workflows with a corresponding domain of a plurality of domains in an Identity System, each domain of said plurality of domains comprising one or more entities and each workflow of said plurality of workflows using a different predefined set of steps to perform a certificate related action affecting validity of the certificate, the certificate comprising a security credential, wherein each workflow in said plurality of workflows corresponds to a different set of characteristics for a user, wherein the first workflow contains a first set of steps and a second workflow in said plurality of workflows contains a second set of steps, wherein said first set of steps is different from said second set of steps, wherein said first workflow calls for obtaining an approval before performing a certificate related action for users having a first user type, and wherein said second workflow does not call for obtaining an approval before performing a certificate related action for users having a second user type;

receiving at the Identity System a request for a first certificate related action for a first user wherein the first certificate related action is selected from a group consisting of a certificate enrollment action, a certificate renewal action, and a certificate revocation action;

determining from said plurality of domains a domain that includes said user;

determining from said plurality of workflows, one or more workflows associated with said domain and capable of performing said certificate related action;

retrieving by the Identity System from said one or more workflows associated with said domain a first workflow for responding to said request wherein retrieving the first workflow comprises selecting the first workflow from the one or more workflows associated with said domain based on the first certificate related action and a user type of the first user from a set of characteristics for the first user from an identity profile for the first user maintained by the Identity System being the first user type and wherein the request includes an identification of said identity profile for the first user;

performing said first workflow, wherein performing said first workflow comprises executing said predefined set of steps of said first workflow to perform said certificate related action including retrieving an approval response from an entity associated with the first user and identified in the identity profile for the first user and obtaining a certificate and a real time status for the certificate from a certificate authority based on the approval response; and

storing the certificate and said real time status in the Identity System, wherein the certificate authority is external to the Identity System..

28.-30. (Canceled)

31. (Previously Presented) The apparatus of claim 27, wherein said method further comprises:

receiving said plurality of workflows.

32. (Previously Presented) The apparatus of claim 27, wherein said method further comprises:

receiving at the Identity System a second request for a second certificate related action for a second user wherein the second certificate related action is selected from a group consisting of a certificate enrollment action, a certificate renewal action, and a certificate revocation action;

determining by the Identity System from said plurality of domains a domain that includes said second user;

determining by the Identity System from said plurality of workflows, one or more workflows associated with said domain that includes said second user and capable of performing said second certificate related action;

retrieving by the Identity System from said one or more workflows associated with said domain that includes the second user a second workflow for responding to said second request, wherein retrieving the second workflow further comprises selecting the second workflow from the one or more workflows associated with said domain that includes said second user based on the second certificate related action and a user type of the second user from a set of

characteristics for the second user from an identity profile for the second user maintained by the Identity System being the second user type, and wherein the second request includes an identification of said identity profile of the second user; and

performing said second workflow, wherein performing said second workflow comprises executing said predefined set of steps of said second workflow to perform said certificate related action including obtaining a second certificate without retrieving an approval response.

33. (Previously Presented) The apparatus of claim 32, wherein said first certificate related action is a certificate enrollment action and said second certificate related action is a certificate enrollment action.

34. (Previously Presented) The apparatus of claim 27, wherein said method further comprises:

performing said first workflow, wherein said first certificate related action is a certificate enrollment action and wherein performing said first workflow comprises:

obtaining a certificate, wherein obtaining the certificate comprises:

authenticating said first user;

forwarding said request to a Certificate Processing Server;

receiving said certificate; and

storing said certificate.

35. (Previously Presented) The apparatus of claim 27, wherein said method further comprises:

performing said first workflow, wherein said first certificate related action is a certificate renewal action and wherein performing said first workflow comprises:

obtaining a certificate, wherein obtaining the certificate comprises:

authenticating said first user;

forwarding said request to a Certificate Processing Server; and

receiving a certificate renewal acknowledgement.

36. (Previously Presented) The apparatus of claim 27, wherein said method further comprises:

performing said first workflow, wherein said first certificate related action is a certificate revocation action and wherein performing said first workflow comprises:

revoking a certificate, wherein revoking the certificate comprises:

authenticating said first user; and

forwarding said request to a Certificate Processing Server.

37-52. (Canceled)

53. (Previously Presented) The method of claim 1, wherein obtaining an approval response comprises applying a Lightweight Directory Access Protocol (LDAP) filter to attributes of the identity profile for the first user.

54. (Previously Presented) The method of claim 9, wherein the entity associated with the first user comprises a third user.

55. (Previously Presented) The method of claim 1, further comprising:

storing validation information for said certificate in the Identity System, wherein said validation information includes an identifier of a time said real time status was retrieved and a validation interval for said real time status;

receiving at the Identity System a request to export the certificate;

determining with the Identity System whether to check a status for said certificate, wherein determining whether to check the status for the certificate comprises querying a parameter field in the Identity System; and

in response to determining to check the status for said certificate, determining with the Identity System whether to check the status for the certificate in real time, wherein determining whether to check the status for the certificate in real time comprises querying a parameter field in the Identity System.

56. (Previously Presented) The one or more processor readable storage devices of claim 16, wherein the method further comprises:

storing validation information for said certificate in the Identity System, wherein said validation information includes an identifier of a time said real time status was retrieved and a validation interval for said real time status;

receiving at the Identity System a request to export the certificate;

determining with the Identity System whether to check a status for said certificate, wherein determining whether to check the status for the certificate comprises querying a parameter field in the Identity System; and

in response to determining to check the status for said certificate, determining with the Identity System whether to check the status for the certificate in real time, wherein determining whether to check the status for the certificate in real time comprises querying a parameter field in the Identity System.

57. (Previously Presented) The apparatus of claim 27, wherein said method further comprises:

storing validation information for said certificate in the Identity System, wherein said validation information includes an identifier of a time said real time status was retrieved and a validation interval for said real time status;

receiving at the Identity System a request to export the certificate;

determining with the Identity System whether to check a status for said certificate, wherein determining whether to check the status for the certificate comprises querying a parameter field in the Identity System; and

in response to determining to check the status for said certificate, determining with the Identity System whether to check the status for the certificate in real time, wherein determining whether to check the status for the certificate in real time comprises querying a parameter field in the Identity System.